



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/621,927	07/17/2003	Paul Anthony Ashley	AUS920030169US1	3074

65362 7590 06/28/2007
INTERNATIONAL BUSINESS MACHINES CORPORATION
c/o HAMILTON & TERRILE, LLP
P.O. BOX 203518
AUSTIN, TX 78720

EXAMINER

HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

06/28/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/621,927

Applicant(s)

ASHLEY ET AL.

Examiner

Brandon S. Hoffman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 April 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-33 are pending in this office action.
2. Applicant's arguments, filed April 9, 2007, have been considered and are persuasive. However, a new ground of rejections is made.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 21-30 and 33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 21-30 and 33 are not limited to tangible embodiments. In view of applicants' disclosure, specification, page 29, lines 26-30, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., EPROM, floppy disc) and intangible embodiments (e.g., transmission-type media, communications links). As such, the claim is not limited to statutory subject matter and is therefore non-statutory.
5. Examiner suggests making the limitation cite a computer readable storage medium, thereby restricting the media to only that which is capable of storing data.

Claim Rejections - 35 USC § 102

6. Claims 1, 2, 11, 12, 21, and 22 are rejected under 35 U.S.C. 102(b) as being anticipated by Freiss et al. (Implementing certificate based authentication for remote

Art Unit: 2136

users with Firewall-1/SecuRemote and openssl as CA, wayback machine archive from January 26, 2002), as evidenced by Wikipedia reference for Transport Layer Security.

Regarding claims 1, 11, and 21, Freiss et al. teaches a method/apparatus/computer program product in a computer-readable medium for performing authentication operations, the method/apparatus/computer program product comprising:

- Performing a non-certificate-based authentication operation through an SSL (Secure Sockets Layer) session between a server and a client (page 1, step 1 through page 2, step 2 and step 3); and
- Subsequent to performing the non-certificate-based authentication operation, performing a certificate-based authentication operation through the SSL session between the server and the client without exiting or renegotiating the SSL session prior to completion of the certificate-based authentication operation (page 2, step 4 through page 4, step 8).

Regarding claims 2, 12, and 22, Freiss et al. teaches wherein negotiation of the SSL session uses a first digital certificate from the client, wherein the certificate-based authentication operation uses a second digital certificate from the client, and wherein the first digital certificate and the second digital certificate are not identical (page 1, step 1, set up of openssl involves a first certificate from the user, see page 2, bullet number 4 from Wikipedia, and page 2, step 4 through page 4, step 8, the creation of a certificate

for the certificate based authentication).

Claim Rejections - 35 USC § 103

7. Claims 3-10, 13-20, and 23-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freiss et al. (Implementing certificate based authentication for remote users with Firewall-1/SecuRemote and openssl as CA, wayback machine archive from January 26, 2002) in view of Joshi et al. (U.S. Patent Pub. No. 2002/0091798).

Regarding claims 3, 13, and 23, Freiss et al. teaches all the limitations of claims 1, 11, and 21, respectively above. However, Freiss et al. does not teach further comprising providing access to a first resource for a client by a server in association with the non-certificate-based authentication operation.

Joshi et al. teaches further comprising providing access to a first resource for a client by a server in association with the non-certificate-based authentication operation (fig. 22, ref. num 795).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine providing access to a first resource during the non-certificated based authentication, as taught by Joshi et al., with the method/apparatus/computer program product of Freiss et al. It would have been obvious for such modifications because the SSL connection provides security of

resources for transmittal to clients.

Regarding claims 4, 14, and 24, Freiss et al. as modified by Joshi et al. teaches wherein the step of providing access to the first resource further comprises:

- Receiving at the server a first resource request from the client (see fig. 22, ref. num 750 of Joshi et al.);
- In response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request, establishing an SSL (Secure Sockets Layer) session between the server and the client (see fig. 22, ref. num 756 of Joshi et al.); and
- In response to successfully performing the non-certificate-based authentication operation between the server and the client through the SSL session, sending a first resource response from the server to the client (see fig. 22, ref. num 790, 792, 794, and 795 of Joshi et al.).

Regarding claims 5, 15, and 25, Freiss et al. teaches all the limitations of claims 1, 11, and 21, respectively above. However, Freiss et al. does not teach further comprising providing access to a second resource for a client by a server in association with the certificate-based authentication operation.

Joshi et al. teaches further comprising providing access to a second resource for a client by a server in association with the certificate-based authentication operation (fig. 35).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine providing access to a second resource during the certificate-based authentication, as taught by Joshi et al., with the method/apparatus/computer program product of Freiss et al. It would have been obvious for such modifications because certificate-based authentication provides additional security of resources for transmittal of secret data to clients.

Regarding claims 6, 16, and 26, Freiss et al. as modified by Joshi et al. teaches wherein the step of providing access for the second resource further comprises:

- Receiving at the server a second resource request from the client through the SSL session (see fig. 35, ref. num 1348 of Joshi et al.);
- In response to determining that the second resource request requires a certificate-based authentication procedure, downloading an executable module to the client from the server through the SSL session (see paragraph 0202 of Joshi et al.);
- Receiving at the server a digital signature that has been generated by the executable module using a digital certificate at the client (see fig. 35, ref. num 1360-1364 of Joshi et al.); and

- In response to successfully verifying the digital signature at the server, sending a second resource response from the server to the client (see fig. 35, ref. num 1366 of Joshi et al.).

Regarding claims 7, 17, and 27, Freiss et al. as modified by Joshi et al. teaches wherein the step of providing access for the second resource further comprises:

- Receiving at the server a second resource request from the client through the SSL session (see fig. 35, ref. num 1348 of Joshi et al.);
- In response to determining that the second resource request requires a certificate-based authentication procedure, triggering execution of a downloadable software module at the client by the server through the SSL session (see paragraph 0204 of Joshi et al.);
- Receiving at the server a digital signature that has been generated by the execution of the downloadable software module using a digital certificate at the client (see fig. 35, ref. num 1360-1364 of Joshi et al.); and
- In response to successfully verifying the digital signature at the server, sending a second resource response from the server to the client (see fig. 35, ref. num 1366 of Joshi et al.).

Regarding claims 8, 18, and 28, Freiss et al. teaches all the limitations of claims 1, 11, and 21, respectively above. However, Freiss et al. does not teach further

comprising obtaining access to a second resource at a server by a client in association with the certificate-based authentication operation.

Joshi et al. teaches further comprising obtaining access to a second resource at a server by a client in association with the certificate-based authentication operation (fig. 35, ref. num 1366).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine providing access to a second resource during the certificate-based authentication, as taught by Joshi et al., with the method/apparatus/computer program product of Freiss et al. It would have been obvious for such modifications because certificate-based authentication provides additional security of resources for transmittal of secret data to clients.

Regarding claims 9, 19, and 29, Freiss et al. as modified by Joshi et al. teaches wherein the step of obtaining access to the second resource further comprises:

- Sending a second resource request from the client to the server through the SSL session (see fig. 35, ref. num 1348 of Joshi et al.);
- Receiving an executable module at the client from the server through the SSL session, wherein the executable module comprises functionality for performing a certificate-based authentication operation (see paragraph 0203 of Joshi et al.);

Art Unit: 2136

- Sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client (see fig. 35, ref. num 1360-1366 of Joshi et al.); and
- Receiving a second resource response from the server at the client (see fig. 35, ref. num 1366 of Joshi et al.).

Regarding claims 10, 20, and 30, Freiss et al. as modified by Joshi et al. teaches wherein the step of obtaining access to the second resource further comprises:

- Sending a second resource request from the client to the server through the SSL session (see fig. 35, ref. num 1348 of Joshi et al.);
- Receiving at the client from the server through the SSL session a response message having content with an associated content type indicator (see paragraph 0214 of Joshi et al.);
- In response to determining a content type for the content, executing a downloadable software module at the client (see paragraph 0214 of Joshi et al.);
- Sending to the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client (see fig. 35, ref. num 1360-1364 of Joshi et al.); and
- Receiving a second resource response from the server at the client (see fig. 35, ref. num 1366 of Joshi et al.).

Regarding claims 31-33, Freiss et al. teaches a method/apparatus/computer program product in a computer-readable medium for performing authentication operations, the method/apparatus/computer program product comprising:

- In response to determining that the first resource request requires completion of a non-certificate-based authentication operation prior to responding to the first resource request, establishing an SSL (Secure Sockets Layer) session between the server and the client (page 1, step 1 through page 2, step 2 and step 3);
- Performing a non-certificate-based authentication operation through the SSL session (page 1, step 1 through page 2, step 2 and step 3); and
- In response to determining that the second resource request requires a certificate-based authentication procedure, downloading an executable module to the client from the server through the SSL session (page 2, step 4 through page 4, step 8).

Freiss et al. does not teach receiving at a server a first resource request from a client; in response to successfully performing the non-certificate-based authentication operation, sending a first resource response from the server to the client; receiving at the server a second resource request from the client through the SSL session subsequent to performing the non-certificate-based authentication operation; receiving at the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client; and in response to

Art Unit: 2136

successfully verifying the digital signature at the server, sending a second resource response from the server to the client.

Joshi et al. teaches receiving at a server a first resource request from a client (fig. 22, ref. num 750); in response to successfully performing the non-certificate-based authentication operation, sending a first resource response from the server to the client (fig. 22, ref. num 795); and receiving at the server a second resource request from the client through the SSL session subsequent to performing the non-certificate-based authentication operation (fig. 35, ref. num 1348); receiving at the server through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client (fig. 35, ref. num 1360-1364); and in response to successfully verifying the digital signature at the server, sending a second resource response from the server to the client (fig. 35, ref. num 1366).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine stuff, as taught by Joshi et al., with the method/apparatus/computer program product of Freiss et al. It would have been obvious for such modifications because the SSL connection provides security of resources for transmittal to clients and certificate-based authentication provides additional security of resources for transmittal of secret data to clients.

Art Unit: 2136

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


6,23,07